An Online Secret Sharing Scheme which Identifies All Cheaters

Chan Yeob Yeun*, Chris J. Mitchell, Mike Burmester

Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
{c.yeun,c.mitchell,m.burmester}@rhbnc.ac.uk

Abstract. A new scheme for computationally secure "online secret sharing" is presented, in which the shares of the participants can be reused. The security of the scheme is based on the intractability of factoring. This scheme has the advantage that it detects cheating and enables the identification of *all* cheaters, regardless of their number, improving on previous results by Pinch and Ghodosi *et al.*

1 Introduction

A secret sharing scheme is a protocol in which a dealer distributes shares of a secret among a set of participants such that only sets of participants belonging to an access structure can recover the secret at a later time. Secret sharing schemes were independently invented in 1979 by Blakley [1] and Shamir [8]. In 1988, Tompa and Woll [9] demonstrated that Shamir's original (t, n) threshold scheme is vulnerable to cheating. That is, the last participant of an authorised set can always cheat the other participants during the reconstruction of the secret, without being detected. As a result the dishonest participant obtains the true secret while the other participants obtain a false one.

Cachin [2] proposed a protocol for online secret sharing for general access structures, in which all the shares are as short as the secret. The scheme provides the capability to share multiple secrets and to dynamically add or remove participants online, without having to redistribute new secret shares to current participants. These additional features are obtained by storing authentic (but not secret) information at a publicly accessible location such as a notice board.

Pinch [6] pointed out that Cachin's scheme does not allow the shares to be reused after the secret has been reconstructed without a further distributed computation, as in Goldreich *et al.* [4]. Pinch presented a protocol for online multiple secret sharing, based on the intractability of the Diffie-Hellman problem, in which the shares can be reused. Ghodosi *et al.* [3] pointed out that Pinch's scheme is also vulnerable to cheating. They presented a modified version of Pinch's protocol which detects and prevents cheating, under the assumption that

* The author is supported by a Research Studentship and Maintenance Award from RHBNC.

a majority of the participants of the authorised reconstruction set are honest. However this scheme does not protect a minority of participants of the authorised set from a colluding majority, who falsely accuses the minority of cheating.

We propose a computationally secure online secret sharing scheme which is based on the intractability of the factoring problem. Compared to Pinch's scheme, and its modification by Ghodosi *et al.*, our scheme has the following advantages: it detects cheating and enables the identification of *all* cheaters by an arbitrator, regardless of their number. The scheme does not rely on a "last participant" who reconstructs the secret on behalf of a minimal trusted set of participants: the responsibility is diffused among all participants.

The proposed scheme has potential practical applications in situations where the participants, the access rules, or the secret itself frequently change. No new shares have to be distributed secretly when new participants join the system or participants leave. Such situations often arise in key management, escrowed encryption systems, and so forth.

2 Preliminaries

A secret sharing scheme is a protocol involving a set $\mathcal{P} = \{P_1, \ldots, P_n\}$ of participants and a dealer D, where $D \notin \mathcal{P}$. Let $\Gamma \subset 2^{\mathcal{P}}$ be an access structure. The dealer D chooses a secret K and distributes privately to each participant $P_i \in \mathcal{P}$ a share S_i of K such that: (i) any authorised set $X \in \Gamma$ can reconstruct the secret K from its shares, (ii) no unauthorised set $X \notin \Gamma$ can do so. Let $\Gamma^* \subset \Gamma$ be the set of *minimal* authorised sets, that is, of sets X such that: $Y \subseteq X$ and $Y \in \Gamma$ implies that $Y = X$.

Let $N = pq$ be the product of two large primes p and q, and let e $(1 < e < \phi(N))$ be chosen so that $(e, \phi(N)) = 1$, where $\phi(N) = (p-1)(q-1)$. The values N and e are public, and the values p, q and $\phi(N)$ are secret. Throughout this paper we work within the multiplicative group of integers modulo N, and we shall assume that factoring N is infeasible [7].

In the secret sharing schemes we will describe below we shall make use of a one-way hash-function f which is collision-resistant. For further information see Sections 9.2 and 9.7 of [5]. In order to identify all cheaters, every participant will use an agreed digital signature scheme, and must have selected a private/public key pair for this scheme. Moreover, every participant must have a means of obtaining a verified copy of the public signature verification key of every other participant. This could, for example, be provided by having a Trusted Third Party (e.g. the dealer, D) certify the public key of every participant, and having every participant distribute their certificate with every signed message they send.

3 A secret sharing protocol

We now present a new secret sharing protocol in which the participants of an authorised set compute the secret K by combining their secret shares in encrypted form. In this way the participants will not reveal their secret shares during the

process of recovering K. The protocol uses a publicly accessible location, e.g. a notice board, where the dealer can store non-forgeable information accessible to all participants. This location will, at least, indicate the number of participants n and the access structure Γ.

The basic protocol to share the secret K is as follows:
First the dealer D selects N and e, and randomly chooses secret shares $S_i < N$, $1 \leq i \leq n$. Then D transmits to each P_i over a secure channel the share S_i, and securely stores S_i for subsequent use to identify cheaters, if cheating is detected. For each minimal authorised set $X \in \Gamma^*$ the dealer D uses e and N to compute

$$T_X = K \oplus f(\textstyle\prod_{x:P_x \in X} S_x^e \bmod N),$$

where $\oplus$ denotes exclusive-or of bit-strings. The dealer D posts the following items on the notice board: the four-tuple (X, e, N, T_X) for every $X \in \Gamma^*$, and the value $f(K)$.
A minimal authorised set $X \in \Gamma^*$ of participants can compute K by performing the following steps:

1. Each participant $P_i \in X$ reads $f(K)$ and the values e, N, T_X from the four-tuple corresponding to the appropriate set X on the notice board. Then P_i computes $S_i^e \bmod N$ and signs the data $(S_i^e \bmod N, X, e, N)$ using his/her private signature key to form $s_{P_i} = sign_{P_i}(S_i^e \bmod N||X||e||N)$, where $||$ denotes concatenation of data items. Finally, $S_i^e \bmod N$ and s_{P_i} are sent by each participant P_i to all the other participants in X.
2. Each participant $P_i \in X$ verifies all the signatures it has received, by using the public keys of the senders, and then computes
$$V_X = \textstyle\prod_{x:P_x \in X} S_x^e \bmod N.$$
3. Each participant $P_i \in X$ reads T_X from the notice board and reconstructs K as follows:
$$K = T_X \oplus f(V_X).$$

One can easily verify the completeness of the protocol: every authorised subset $X \in \Gamma$ will recover K.

A generalisation of this scheme can be used to share multiple secrets K_h, $h = 1, 2, \ldots, m$. It is possible to use the same one-way hash-function f and the *same* set of secret shares $S_1, S_2, \ldots, S_n$ to share all the secrets K_h. Whenever a new secret K_h is to be shared, the access structure may be different to that used for previous secrets, and hence we denote the access structure for secret K_h by Γ_h. For each secret K_h the dealer D chooses a fresh pair (e_h, N_h), where it is essential that D chooses a distinct modulus N_h for every secret K_h. For each $X \in \Gamma_h$ the dealer computes

$$T_{X,h} = K_h \oplus f(\textstyle\prod_{x:P_x \in X} S_x^{e_h} \bmod N_h), \quad h = 1, 2, \ldots, m$$

and publishes the following items on the notice board:

$$(X, e_h, N_h, T_{X,h}) \text{ and } f(K_h), \quad h = 1, 2, \ldots, m.$$

The reconstruction of the secret is as before.

The properties of well-chosen pairs (e_h, N_h) and the function f, ensure that the reuse of the set of secret shares $S_1, S_2, \ldots, S_n$ does not leak any information which may be useful to cheaters and/or other malicious users.

4 Analysis of the protocol

The proposed protocol described in the previous section has the following properties.

4.1 How cheating may occur

In both the proposed protocol and its generalisation to multiple secrets it is possible for one of the participants to cheat the others in such a way that the cheater will get the correct secret but the other participants do not.

Suppose that participant P_j contributes a fake encrypted share S' instead of $S_j^e \bmod N$. Then every participant of the authorised set X will compute V_X incorrectly as $V'_X = S' \cdot \prod_{x \neq j : P_x \in X} S_i^e \bmod N$ instead of $V_X = \prod_{x : P_x \in X} S_i^e \bmod N$. However P_j, who knows $S_j^e \bmod N$, can calculate the correct secret V_X.

4.2 How to detect cheating

In the initialisation phase of the scheme, the dealer D publishes $f(K_h)$ on the notice board for every secret K_h that is being shared. Every participant, having reconstructed the secret (K'_h, say), can verify its validity by hashing it and comparing the resulting hashed value $f(K'_h)$ with the value on the notice board. If the verification fails, then most probably cheating has occurred in the protocol and thus the computed secret is not correct. This test detects cheating but does not identify the cheater(s). We now show how to identify *all* the cheaters.

4.3 How to identify all cheaters

In the event of cheating having been detected by the method just described, the participants in the authorised set X can appeal to the dealer D to help discover the identity of the cheaters. Notice that the dealer will only be involved in arbitration *after cheating* has been detected, and will not need to be actively involved in the normal operation of the reconstruction phase of the scheme.

In order to identify *all* cheaters, every participant $P_i \in X$ sends to the dealer the data received during execution of the protocol, signed with their private key. The dealer verifies the signed data received from each P_i, and compares the submitted value of $S_i^e \bmod N$, with that computed by using the stored value of the share S_i. If a submitted value is different from the calculated value, then most probably P_i cheated. P_i cannot claim to have been framed, since D has P_i's signature s_{P_i} on $(S_i^e \bmod N || X || e || N)$. Therefore, the dealer will be able to identify *all* the parties who sent incorrect values during the protocol.

This use of signatures will also protect a minority of participants of an authorised set from a colluding majority who falsely accuses the minority of cheating.

5 Conclusion

We have presented a scheme which allows the reconstruction of an arbitrary number of secrets and provides the capability to dynamically add or remove participants online, without having to redistribute new shares secretly to current participants by storing additional authentic (but not secret) information on the notice board.

In addition, this scheme can be used in such a way that cheating by participants will be detected, in which case the participants of an authorised set X can request help from the dealer D, who can always uniquely identify the cheaters.

6 Acknowledgements

The authors are grateful to Fred Piper for his support, and to Peter Wild and Karl Brincat for comments on an early draft of the paper.

References

1. G.R. Blakley. Safeguarding cryptographic keys. In *Proceedings of AFIPS National Computer Conference*, pp. 313–317, 1979.
2. C. Cachin. On-line secret sharing. In C. Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding*, pp. 190–198. Springer-Verlag, 1995.
3. H. Ghodosi, J. Pieprzyk, G.R. Chaudhry, and J. Seberry. How to prevent cheating in Pinch's scheme. *Electronics Letters*, 33(17):1453–1454, 1997.
4. O. Goldreich, S. Micali, and A. Widgerson. How to play any mental game or a completeness theorem for protocols with honest majority. In *Proceedings of 19th ACM Symposium on the Theory of Computing*, pp. 218–229, 1987.
5. A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.
6. R.G.E. Pinch. Online multiple secret sharing. *Electronics Letters*, 32(12):1087–1088, 1996.
7. R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.
8. A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.
9. M. Tompa and H. Woll. How to share a secret with cheaters. *Journal of Cryptology*, 1:133–138, 1988.